AMENDMENTS TO CLAIMS:

The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A method for authorizing a user on a computer network using chained mapping records, the method including:

receiving a digital certificate for a user requesting access to said computer network;

comparing a distinguished name or a partial distinguished name corresponding to the digital certificate with a plurality of mapping records;

replacing a variable from a first matching mapping record with an environmental factor to create a first search criteria, the first matching mapping record indicating the distinguished name or the partial distinguished name, wherein the environmental factor includes one or more system or application statuses in effect at the time the user signs-on the computer network, operable for enabling the first matching mapping record to point to multiple user identifications;

comparing the first search criteria with the plurality of mapping records; and

generating an authorization indicator responsive to at least one of comparing the distinguished name or a partial distinguished name and comparing the first search criteria with the plurality of mapping records.

2. (Previously Presented) The method of claim 1, wherein the generating an authorization indicator includes generating a security context control block using a user identification from a second matching mapping record, the second matching mapping record indicating the first search criteria.

3. (Previously Presented) The method of claim 1, further including:

replacing a variable from a second matching mapping record with the environmental factor to create a second search criteria, the second matching mapping record indicating the first search criteria.

4. (Previously Presented) The method of claim 3, wherein the generating an authorization indicator includes generating a security context control block using a user identification from a

third matching mapping record, the third matching mapping record indicating the second search criteria.

5. (Original) The method of claim 1, further including:

eliminating a portion of an X.500 distinguished name to create the partial distinguished name used in said comparing the partial distinguished name with the plurality of mapping records.

6. (Previously Presented) The method of claim 1, wherein the generating an authorization indicator includes generating a security context control block using a user identification from the first matching mapping record if the first matching mapping record includes the user identification.

7. (Previously Presented) The method of claim 1, wherein comparing the distinguished name or the partial distinguished name corresponding to the user with a plurality of mapping records includes comparing an X.500 distinguished name of the user with the plurality of mapping records.

8. (Previously Presented) The method of claim 1, wherein the environmental factor includes a system status existing at the time the user signs-on the computer network and replacing a variable includes replacing the variable from the first matching mapping record with said system status.

9. (Currently Amended) A system for authorizing a user on a computer network using chained mapping records, the system including:

a digital certificate means for receiving a distinguished name over said computer network, said distinguished name corresponding to the user;

a distinguished name mapping record within a directory database, said distinguished name mapping record indicative of at least a portion of said distinguished name, said distinguished name mapping record including a first data field, said first data field including a first variable indicative of a first environmental factor, wherein the first environmental factor

includes one or more system or application statuses in effect at the time said digital certificate is received, operable for enabling said first matching mapping record to point to multiple user identities;

a first criteria mapping record corresponding to a first state of said first environmental factor, said first criteria mapping record including a second data field, said second data field including a first user identity; and

a mapping process configured to receive said digital certificate, wherein said mapping process generates a security context control block using said first user identity in response to said first state of said first environmental factor;

wherein said digital certificate means is on a computer readable medium.

10. (Original) The system of claim 9, further including:

a second criteria mapping record corresponding to a second state of said first environmental factor, said second criteria mapping record including a third data field, said third data field including a second user identity; and

wherein said mapping process is further configured to generate a security context control block using said second user identity in response to said second state of said first environmental factor.

11. (Original) The system of claim 9, further including:

a second criteria mapping record corresponding to a second state of said first environmental factor, said second criteria mapping record including a third data field, said third data field including a second variable indicative of a second environmental factor;

a third criteria mapping record corresponding to said second environmental factor, said third criteria mapping record including a fourth data field, said fourth data field including a second user identity; and

wherein said mapping process is further configured to generate a security context control block using said second user identity in response to said second state of said first environmental factor and said third environmental factor.

12. (Original) The system of claim 9, wherein said distinguished name is an X.500 distinguished name.

13. (Original) The system of claim 10, wherein said first user identity represents a first level of network authorization, and said second user identity represents a second level of network authorization.

14. (Original) The system of claim 9, wherein said first environmental factor is a network status at the time said digital certificate is received by said mapping process.

15. (Original) The system of claim 9, wherein said first environmental factor is an application status at the time said digital certificate is received by said mapping process.

16. (Original) The system of claim 9, wherein said first environmental factor is included in said digital certificate.

17. (Previously Presented) A storage medium encoded with machine-readable computer program code for authorizing a user on a computer network using chained mapping records, the storage medium including instructions for causing a computer to implement a method comprising:

comparing a distinguished name or a partial distinguished name corresponding to the user with a plurality of mapping records;

replacing a variable from a first matching mapping record with an environmental factor to create a first search criteria, the first matching mapping record indicating the distinguished name or the partial distinguished name, wherein the environmental factor includes one or more system or application statuses in effect at the time the user signs-on on the computer network, operable for enabling the first matching mapping record to point to multiple user identifications;

comparing the first search criteria with the plurality of mapping records; and generating an authorization indicator responsive to at least one of comparing the distinguished name or a partial distinguished name and comparing the first search criteria with the plurality of mapping records.

18. (Previously Presented) The storage medium of claim 17, wherein the generating an authorization indicator includes generating a security context control block using a user identification from a second matching mapping record, the second matching mapping record indicating the first search criteria.

19. (Previously Presented) The storage medium of claim 17, further comprising instructions for causing a computer to implement:

replacing a variable from a second matching mapping record with the environmental factor to create a second search criteria, the second matching mapping record indicating the first search criteria.

20. (Previously Presented) The storage medium of claim 19, wherein the generating an authorization indicator includes generating a security context control block using a user identification from a third matching mapping record, the third matching mapping record indicating the second search criteria.

21. (Original) The storage medium of claim 17 further comprising instructions for causing a computer to implement:

eliminating a portion of an X.500 distinguished name to create the partial distinguished name used in said comparing the partial distinguished name with the plurality of mapping records.

22. (Previously Presented) The storage medium of claim 17, wherein the generating an authorization indicator includes generating a security context control block using a user identification from the first matching mapping record if the first matching mapping record includes the user identification.

23. (Previously Presented) The storage medium of claim 17, wherein comparing the distinguished name or the partial distinguished name corresponding to the user with a plurality of

mapping records includes comparing an X.500 distinguished name of the user with the plurality of mapping records.

24. (Previously Presented) The storage medium of claim 17, wherein the environmental factor includes a system status existing at the time the user signs-on the computer network and replacing a variable includes replacing the variable from the first matching mapping record with said system status.